CA Single Sign-On

Versionshinweise

r12.0

CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden CA-Produkte:

- CA® Single Sign-On CA SSO
- CA® Access Control
- CA® ACF2
- CA® Audit
- CA® Directory
- CA® Top Secret
- Unicenter® Software Delivery

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Inhalt

Kapitel 1: Willkommen

Willkommen bei CA Single Sign-On (CA SSO). Dieses Dokument enthält Informationen zur Produktinstallation, zur Betriebssystemunterstützung, zu neuen Funktionen, zu Änderungen vorhandener Funktionen, zu bekannten Problemen, zu Drittanbieter-Lizenzen sowie darüber, wie Sie sich mit dem technischen Support von CA in Verbindung setzen können.

Kapitel 2: Neue Funktionen

Dieses Kapitel enthält folgende Themen:

Vista-Unterstützung für den CA SSO-Client

Der CA SSO-Client wird unter Windows Vista unterstützt. Vista verwaltet Anwendungen anders als andere Plattformen, daher verhält sich auch der CA SSO-Client anders, wenn Sie versuchen, Anwendungen zu starten.

Unter Vista werden Anwendungen als Standardanwendungen und Anwendungen mit erhöhten Rechten klassifiziert. *Standardanwendungen* sind Anwendungen, von denen keine Systemdateien geändert oder geschrieben werden müssen. Dazu gehören auch die Registrierung und der Ordner "Programme". *Anwendungen mit erhöhten Rechten* sind Anwendungen, von denen Systemdateien mit Zugriffsbeschränkung geändert oder geschrieben werden müssen. Als Standardbenutzer unter Vista können Sie nur Standardanwendungen ausführen. Möchten Sie Anwendungen mit erhöhten Rechten ausführen, benötigen Sie Administratorrechte.

Hinweis: Weitere Informationen zum Verhalten des CA SSO-Clients unter Vista finden Sie im *CA SSO-Administrationshandbuch* und in der *Online-Hilfe für den CA SSO-Client*.

SSO-Anmeldeinformationsanbieter für Vista

Beim Betriebssystem Vista werden zwei neue SSO-Anmeldeinformationsanbieter installiert. Einer der neuen Anmeldeinformationsanbieter bietet Unterstützung für die interaktive Workstationanmeldung mit Hilfe von lokalen oder SSO-Authentifizierungsmethoden, der andere Anmeldeinformationsanbieter hilft dem Benutzer, sich direkt bei der Windows-Workstation anzumelden. Wenn sich Benutzer bei einem Windows Vista-Computer anmelden, geben sie ihre Anmeldeinformationen unter Verwendung des SSO-Anmeldeinformationsanbieters ein. Wenn das Betriebssystem Vista ist, zeigt das SSO-Installationsprogramm nur Vista-Funktionen an. Alle anderen Plattformfunktionen werden ausgeblendet. So wird beispielsweise im Dialogfeld für die verfügbaren Funktionen GINA durch den Anmeldeinformationsanbieter ersetzt.

Der SSO-Anmeldeinformationsanbieter für Vista stellt zwei neue Modi zum Entsperren von Workstations bereit:

- Modus 4: Sperrungsoption "Einzelner SSO-Benutzer für Windows-Sitzung"
- Modus 5: Sperrungsoption "Mehrere SSO-Benutzer für Windows-Sitzung"

Weitere Informationen zum SSO-Anmeldeinformationsanbieter für Vista und die Modi zum Entsperren von Workstations finden Sie im *CA SSO-Administratorhandbuch*.

Option zum Identifizieren von Anwendungen mit erhöhten Rechten in Vista

Der CA SSO-Client wird unter Vista unterstützt. Vista verwaltet Anwendungen anders als andere Plattformen, daher verhält sich auch der CA SSO-Client anders, wenn Sie versuchen, Anwendungen zu starten.

Unter Vista werden Anwendungen als Standardanwendungen und Anwendungen mit erhöhten Rechten klassifiziert. *Standardanwendungen* sind Anwendungen, von denen keine Systemdateien geändert oder geschrieben werden müssen. *Anwendungen mit erhöhten Rechten* sind Anwendungen, von denen Systemdateien mit Zugriffsbeschränkung geändert oder geschrieben werden müssen. Als Standardbenutzer unter Vista können Sie nur Standardanwendungen ausführen. Möchten Sie Anwendungen mit erhöhten Rechten ausführen, benötigen Sie Administratorrechte.

Um diese Anwendungstypen unter Vista zu berücksichtigen, muss der CA SSO-Client zwischen Standardanwendungen und Anwendungen mit erhöhten Rechten unterscheiden. Der CA SSO-Server ermittelt, ob der SSO-Interpreter im Modus mit erhöhten Rechten ausgeführt werden muss. Hierzu wird das Attribut "Als Administrator ausführen" in den Anwendungseigenschaften herangezogen. Das folgende Attribut wird zum Dialogfeld "Attribute" von Anwendungsressourcen hinzugefügt:

Als Administrator ausführen

Hinweis: Weitere Informationen zum Attribut "Als Administrator ausführen" finden Sie in der Hilfe für CA SSO Policy Manager.

TCL-Tags-Unterstützung für Anwendungen mit erhöhten Rechten

Sobald Sie versuchen, auf eine Anwendung mit erhöhten Rechten unter Vista zuzugreifen, muss der CA SSO-Client ebenfalls in einem Modus mit erhöhten Rechten ausgeführt werden. Zum Ausführen des CA SSO-Clients in einem Modus mit erhöhten Rechten benötigen Sie Administratorrechte. Wenn Sie also versuchen, Anwendungen unter Vista zu starten, werden Sie möglicherweise zweimal aufgefordert, die Administratoranmeldeinformationen anzugeben - einmal zum Ausführen des CA SSO-Clients in einem Modus mit erhöhten Rechten und einmal zum Starten der Anwendung mit erhöhten Rechten. Vista fordert Administratorrechte mit den Eingabeaufforderungen der Benutzerkontensteuerung an.

Unter Vista kann eine Anwendung mit erhöhten Rechten eine andere Anwendung mit erhöhten Rechten ohne Eingabeaufforderungen der Benutzerkontensteuerung starten. Daher kann der CA SSO-Client Anwendungen mit erhöhten Rechten starten, ohne dass Administratorrechte beim Benutzer angefordert werden, wenn der Client selbst in einem Modus mit erhöhten Rechten ausgeführt wird. Sie können den CA SSO-Client so konfigurieren, dass die zweite Eingabeaufforderung der Benutzerkontensteuerung, die zum Starten von Anwendungen mit erhöhten Rechten erforderlich ist, unterdrückt wird. Hierzu konfigurieren Sie die folgenden Tags, die zur TCL-Erweiterung *-sso run* hinzugefügt werden:

- [-elevated y|n]
- [-suppressconsent y|n]

Hinweis: Weitere Informationen zur TCL-Erweiterung -sso run finden Sie im *Referenzhandbuch für TCL-Skripts*.

Änderungen beim Installationsprogramm

Der CA SSO-Client unterstützt Vista. Dementsprechend wurde auch das Installationsprogramm für den CA SSO-Client aktualisiert und unterstützt jetzt ebenfalls Vista. Das Installationsprogramm für den CA SSO-Client beinhaltet eine Version des TCL-Interpreters für Vista, die sich von den TCL-Interpretern für andere Windows-Betriebssysteme unterscheidet. Der TCL-Interpreter für Vista muss im Modus mit erhöhten Rechten ausgeführt werden, um Anwendungen mit erhöhten Rechten unter Vista zu verarbeiten.

Darüber hinaus beinhaltet das Installationsprogramm für den CA SSO-Client einen CA SSO-Anmeldeinformationsanbieter für Vista anstelle von CA SSO-GINA. Wenn Sie den CA SSO-Client installieren, überprüft das Installationsprogramm das zugrunde liegende Betriebssystem und stellt Ihnen die folgenden Optionen zur Wahl, die sich für Vista und andere Betriebssysteme unterscheiden:

Für Vista

SSO-Anmeldeinformationsanbieter

Für andere Windows-Betriebssysteme

SSO-GINA

Änderungen an der Datei Client.ini

Die folgenden Schlüssel wurden zum Abschnitt [GINA] in der Datei client.ini von CA SSO r12 hinzugefügt. Diese Schlüssel steuern den Abruf und die Anzeige von Domänennamen durch GINA.

- FetchDomainsFromSystem
- Domänen

Der folgende Schlüssel wurde zum Abschnitt [CredentialProvider] der Datei client.ini von CA SSO r12 hinzugefügt. Dieser Schlüssel gibt das Standardbild an, das der SSO-Anmeldeinformationsanbieter verwendet.

- LoginBitmap

Ein neuer Abschnitt [CredentialProviderTileImages] mit den folgenden Schlüsseln wurde zur Datei client.ini von CA SSO r12 hinzugefügt. Diese Schlüssel geben die Standardbilder an, die der SSO-Anmeldeinformationsanbieter für verschiedene Authentifizierungsdialogfelder für die RSA-Authentifizierung, Zertifikatauthentifizierung, Windows-Authentifizierung, LDAP-Authentifizierung und so weiter verwendet.

- ServerSetTile
- MSCPTile
- SSOCPTile

- WINCPTile
- LDAPCPTile
- RSACPTile
- CERTCPTile

Hinweis: Weitere Informationen zur Datei client.ini finden Sie im *Administrationshandbuch*.

FIPS 140-2

CA SSO r12 unterstützt FIPS 140-2 bei neuen Installationen und Upgrades. Außerdem gehört zum Lieferumfang von CA SSO ein Befehlszeilenprogramm mit Namen PwdEncUtil, das Folgendes ermöglicht:

- Generieren neuer Schlüssel für die Verschlüsselung von Schlüsseln und Kennwörtern (KEK und PEK) und Beenden bzw. Ersetzen aktiver Schlüssel. (KEK und PEK sind die Schlüssel, die vom SSO-Server gegenwärtig verwendet werden.)
- Verschlüsseln Sie alle vorhandenen Kennwörter nach Ändern des PEK erneut.
- Erneutes Verschlüsseln älterer Kennwörter (nach einem Upgrade von 8.1)

Weitere Informationen zu diesem Dienstprogramm finden Sie im "FIPS 140-2 Appendix" im CA SSO-*Administrationshandbuch*.

IPv6-Unterstützung

Beim Konfigurieren von CA SSO können Sie sowohl IPv4- als auch IPv6-Adressen eingeben.

CA SSO unterstützt IPv6 unter den folgenden Betriebssystemen:

- Vista
- Server 2003 Enterprise Edition und Standard Edition SP2
- XP SP2

Hinweis: Die Windows-Authentifizierungsmethode wird für CA SSO- und GINA-Clients in einer reinen IPv6-Umgebung nicht unterstützt. Diese Einschränkung gilt für Windows XP und Windows 2003 Server.

508-Kompatibilität

Bei dieser Version von CA SSO wurde der SSO-Client aktualisiert, damit er die Standards gemäß "Section 508" in den folgenden Kategorien erfüllt:

- Softwareanwendungen und Betriebssysteme
- Funktionelle Leistungskriterien und Informationen
- Dokumentation
- Support

Weitere Informationen:

Funktionen zur behindertengerechten Bedienung (siehe Seite 45)

Kapitel 3: Änderungen an vorhandenen Funktionen

Dieses Kapitel enthält folgende Themen:

Unterstützung für Webagenten

Bei Verwendung der CA SSO-Webagenten für die formularbasierte Authentifizierung werden diese Agenten in dieser Version nicht bereitgestellt. Verwenden Sie stattdessen die CA SSO r8-Versionen dieser Agenten.

Für den Schutz des Webzugriffs ist CA® SiteMinder Web Access Manager der Upgrade-Pfad der Wahl. Weitere Informationen hierzu erhalten Sie von Ihrem SSO-Support-Mitarbeiter vor Ort.

Abwärtskompatibilität mit CA SSO-Clients

Die folgenden Punkte zur Abwärtskompatibilität müssen vor dem Upgrade von CA SSO r12-Komponenten beachtet werden:

- CA SSO r12-Server sind mit CA SSO r8.1-Clients abwärtskompatibel.
- Der CA SSO r12-Client ist mit früheren Versionen von CA SSO-Komponenten nicht abwärtskompatibel.
- CA SSO r12-Authentifizierungsagenten sind nur mit e12-Clients kompatibel.
- CA SSO r8.1-Clients sind mit r8.1- oder r12-Authentifizierungsagenten kompatibel.

Hinweis: Weitere Informationen zur Abwärtskompatibilität mit CA SSO-Clients finden Sie im *Implementierungshandbuch*.

Aktualisieren von CA SSO-Komponenten

CA SSO r12 unterstützt ein Upgrade aller Komponenten von CA SSO r8.1. CA SSO unterstützt kein direktes Upgrade von r8.0 auf r12. Sie können nur die r8.0-Clientkomponenten direkt auf r12 aktualisieren. Für ein Upgrade von CA SSO r8.0 auf CA SSO r12 haben Sie folgende Möglichkeiten:

- Sie richten eine neue CA SSO r12-Umgebung ein. Dies umfasst Folgendes:
  - Installation der r12-Server
  - Migration aller Daten von r8 auf r12
- Sie aktualisieren auf den r8.1-Server und dann auf den r12-Server.

Sie müssen die Upgrade-Pfade für die Datenmigration verwenden, um sicherzustellen, dass die Daten aus den Benutzer- und Richtlinienspeichern von r8.0 oder r8.1 beim Upgrade in den folgenden Szenarios auf CA SSO r12 aktualisiert werden:

- Der CA SSO-Server ist auf demselben System installiert, aber die Verwendung des Upgrade-Assistenten, zum Beispiel im Szenario eines Upgrades von SSO r8 auf r12, ist nicht möglich.
- Der CA SSO-Server r12 ist auf einem anderen System als der vorhandene 8.0- oder 8.1-Server installiert, und die vorhandene Konfiguration muss auf ein neues System migriert werden.

Hinweis: Weitere Informationen zum Upgrade auf r12 finden Sie im *Implementierungshandbuch*.

Kapitel 4: Unterstützte Betriebssysteme

Im Folgenden wird die Betriebssystemunterstützung für jede Komponente beschrieben.

Dieses Kapitel enthält folgende Themen:

SSO-Server

CA SSO unterstützt nur Serverfarmen, bei denen alle CA SSO-Server auf Computern mit demselben Betriebssystem installiert sind.

Hinweis: Der CA SSO-Server wird auf 64-Bit-UNIX-Plattformen im 32-Bit-Modus ausgeführt. CA SSO unterstützt nur 32-Bit-Windows-Plattformen.

Microsoft Windows

- 2003 Enterprise Edition und Standard Edition SP2
- 2003 Enterprise Edition und Standard Edition SP2 auf VMWare ESX Server 3.5
- 2003 R2 SP2 Enterprise Edition und Standard Edition

SSO-Client

Der CA SSO-Client wird unter den folgenden Betriebssystemen unterstützt:

Microsoft Windows

- Vista SP1
- Server 2003 Enterprise Edition und Standard Edition SP2
- XP SP2
- 2000 Professional, Server und Advanced Server SP4

ADS Listener

Der ADS Listener wird unter den folgenden Betriebssystemen unterstützt:

Microsoft Windows

- 2003 Enterprise Edition und Standard Edition SP2

Authentifizierungsagenten

Authentifizierungsagenten werden unter den folgenden Betriebssystemen unterstützt:

Certificate Agent (Zertifikatagent)

Microsoft Windows

- 2003 Enterprise Edition und Standard Edition SP2
- 2003 Enterprise Edition und Standard Edition SP2 auf VMWare ESX Server 3.5

LDAP Agent (LDAP-Agent)

Microsoft Windows

- 2003 Enterprise Edition und Standard Edition SP2
- 2003 Enterprise Edition und Standard Edition SP2 auf VMWare ESX Server 3.5

RSA Agent (RSA-Agent)

Microsoft Windows

- 2003 Enterprise Edition und Standard Edition SP2
- 2003 Enterprise Edition und Standard Edition SP2 auf VMWare ESX Server 3.5

SSO Agent (SSO-Agent)

Der SSO-Authentifizierungsagent ist Bestandteil des SSO-Servers. Siehe dazu die vom SSO-Server unterstützten Plattformen im vorherigen Thema.

Windows-Agent

Microsoft Windows

- 2003 Enterprise Edition und Standard Edition SP2
- 2003 Enterprise Edition und Standard Edition SP2 auf VMWare ESX Server 3.5

Windows-Kennwortsynchronisierungs-Agent

Dieser Agent wird unter den folgenden Betriebssystemen unterstützt:

Microsoft Windows

- 2003 Enterprise Edition und Standard Edition SP2
- 2003 Enterprise Edition und Standard Edition SP2 auf VMWare ESX Server 3.5

Weitere Informationen zu den Plugin-Spezifikationen für den SSO-Server finden Sie unter SSO-Server (siehe Seite 19).

Policy Manager

Policy Manager wird unter den folgenden Betriebssystemen unterstützt:

Microsoft Windows

- Vista SP1
- 2003 Enterprise Edition und Standard Edition SP2
- XP SP2

Session Administrator (Sitzungsadministrator)

Der Session Administrator (Sitzungsadministrator) wird unter den folgenden Betriebssystemen unterstützt:

Microsoft Windows

- 2003 Enterprise Edition und Standard Edition SP2

Kapitel 5: Systemanforderungen

Im Folgenden werden die Systemvoraussetzungen für jede Komponente beschrieben.

Dieses Kapitel enthält folgende Themen:

SSO-Server

Folgendes sind die minimalen Voraussetzungen für das System, auf dem der CA SSO-Server ausgeführt wird:

- Pentium 2 GHz oder höher
- Mindestens 2 GB RAM
- 2 GB freier Festplattenspeicher
- DVD-ROM-Laufwerk (Das Installationspaket wird nur im DVD-Format bereitgestellt.)
- Aktive Netzwerkverbindung
- TCP/IP

Hinweis: Die Voraussetzungen können je nach Anzahl der Benutzer in Ihrem Datenspeicher und weiteren Variablen variieren. CA empfiehlt die Planung Ihrer Architektur, damit Sie die erforderlichen Größen- und Skalierungsvoraussetzungen Ihrer Server für Ihre Umgebung besser ermitteln können.

SSO-Client

Folgendes sind die minimalen Voraussetzungen für das System, auf dem der CA SSO-Client ausgeführt wird:

- Pentium 266 MHz oder höher
- Mindestens 256 MB RAM
- 200 MB freier Speicherplatz
- DVD-ROM-Laufwerk (Das Installationspaket wird nur im DVD-Format bereitgestellt.)
- Aktive Netzwerkverbindung
- TCP/IP

ADS Listener

Folgendes sind die minimalen Voraussetzungen für das System, auf dem der ADS Listener ausgeführt wird:

- Pentium 512 MHz oder höher
- Mindestens 1 GB RAM
- 500 MB freier Speicherplatz
- DVD-ROM-Laufwerk (Das Installationspaket wird nur im DVD-Format bereitgestellt.)
- Aktive Netzwerkverbindung
- TCP/IP

Authentifizierungsagenten

Folgendes sind die minimalen Voraussetzungen für das System, auf dem die Authentifizierungsagenten ausgeführt werden:

- Pentium 512 MHz oder höher
- Mindestens 512 MB RAM
- 500 MB freier Speicherplatz
- DVD-ROM-Laufwerk (Das Installationspaket wird nur im DVD-Format bereitgestellt.)
- Aktive Netzwerkverbindung
- TCP/IP

Windows-Kennwortsynchronisierungs-Agent

Folgendes sind die minimalen Voraussetzungen für den Windows-Kennwortsynchronisierungs-Agenten:

- Pentium 512 MHz oder höher
- Mindestens 512 MB RAM
- 500 MB freier Speicherplatz
- DVD-ROM-Laufwerk (Das Installationspaket wird nur im DVD-Format bereitgestellt.)
- Aktive Netzwerkverbindung
- TCP/IP

Policy Manager

Folgendes sind die minimalen Voraussetzungen für das System, auf dem Policy Manager ausgeführt wird:

- Pentium 266 MHz oder höher
- 256 MB RAM
- 20 MB freier Speicherplatz
- DVD-ROM-Laufwerk (Das Installationspaket wird nur im DVD-Format bereitgestellt.)
- Aktive Netzwerkverbindung
- TCP/IP

Session Administrator (Sitzungsadministrator)

Folgendes sind die minimalen Voraussetzungen für das System, auf dem der Session Administrator (Sitzungsadministrator) ausgeführt wird:

- Pentium 266 MHz oder höher
- 256 MB RAM
- 20 MB freier Speicherplatz
- DVD-ROM-Laufwerk (Das Installationspaket wird nur im DVD-Format bereitgestellt.)
- Aktive Netzwerkverbindung
- TCP/IP

Kapitel 6: Allgemeine und die Installation betreffende Punkte

Folgendes sollte bei der Installation von CA SSO berücksichtigt werden.

Bei der Größe und Skalierung zu beachten

CA empfiehlt, die Größe und Skalierung Ihrer CA SSO-Umgebung den Anforderungen Ihres Unternehmens entsprechend zu wählen. Von CA werden zu diesem Zweck Tools bereitgestellt. Weitere Informationen finden Sie unter *CA SSO Performance Measurement Module* auf Support Connect.

Beim Installationsprogramm für den SSO-Client zu beachten

Das Installationsprogramm für den SSO-Client verwendet das Windows-Programm cacls.exe, um Verzeichnisberechtigungen festzulegen. Bei diesem Tool besteht ein im Microsoft Knowledge Base-Artikel 834721 beschriebenes Problem. Um dieses Problem zu umgehen, wenden Sie den von Microsoft bereitgestellten Betriebssystem-Hotfix an.

Voraussetzungen für eine unbeaufsichtigte Installation des Clients

Bevor Sie eine unbeaufsichtigte Installation des CA SSO r12-Clients in einer Windows 2000 Server-Betriebsumgebung durchführen, stellen Sie sicher, dass das frei verbreitbare Microsoft Visual C++ 2005-Paket auf dem betreffenden Computer installiert ist.

Bei der SSO-Server-Installation zu beachten

Der SSO-Server kann nicht an einem Speicherort installiert werden, dessen Pfad Nicht-ASCII-Zeichen enthält.

Policy Manager kann keine Verbindung zum SSO-Server herstellen, wenn unterschiedliche Betriebsmodi verwendet werden

Wenn der SSO-Server im gemischten Betriebsmodus installiert wird und Policy Manager im Nur-FIPS-Betriebsmodus installiert wird, kann Policy Manager keine Verbindung zum SSO-Server herstellen.

Ändern Sie die CA Access Control-Registrierungseinträge in den Nur-FIPS-Betriebsmodus. Ändern Sie außerdem den CA SSO-Servermodus in den Nur-FIPS-Betriebsmodus.

Hinweis: Weitere Informationen zum Ändern des Betriebsmodus für CA Access Control und den CA SSO-Server finden Sie im *CA SSO-Implementierungshandbuch*.

Installation beim Upgrade auf den r12-SSO-Server schlägt fehl

Wenn der vorhandene r8.1-Server von r8.0 aktualisiert wurde und dann auf r12 aktualisiert wird, wird die Installation nicht durchgeführt. Führen Sie das Upgrade von r8.0 auf r12 in folgender Reihenfolge durch:

1. Aktualisieren Sie die Ingres-Version von r2.6 auf mindestens r3.0 auf dem Computer mit der r8.0-Serverinstallation.
2. Aktualisieren Sie den SSO-Server von r8.0 auf r8.1.
3. Aktualisieren Sie den SSO-Server von r8.1 auf r12.

Server-Upgrade von r8.1 GA auf r12 wird nicht unterstützt

Beim Upgrade der r8.1 GA-Version des SSO-Servers auf r12 schlägt die Installation fehl.

Um dieses Problem zu umgehen, aktualisieren Sie r8.1 auf r8.1 CR6 oder höher und führen Sie dann das Upgrade auf r12 durch.

Bei der Microsoft Windows-Installation zu beachten

Auf manchen Computern ist der Zeitstempel für die Installations- und Deinstallationsprotokolldatei in GMT-Zeit und nicht in Ortszeit angegeben. Dies ist ein bekanntes Problem bei Java, wenn die Windows-Ländereinstellung und -Zeitzone nicht ordnungsgemäß festgelegt sind.

Um dieses Problem zu umgehen, setzen Sie die Ländereinstellung und Zeitzone Ihres Windows-Systems zurück. Dazu kann Ihre Zeitzone in eine andere Zeitzone geändert und diese angewendet und anschließend wieder die richtige Zeitzone festgelegt werden.

Konfiguration für Client.ini-Dateien nach dem Upgrade

CA SSO verwendet die Einträge "IdentityFile" und "TrustFile" im Abschnitt [Auth.Win] der Datei Auth.ini, um die Verbindung zu einem Windows-Authentifizierungsagenten herzustellen. Die IdentityFile- und TrustFile-Dateien werden bei r12 am folgenden Speicherort gespeichert:

<*Installationsordner*>\ca\Single Sign-On\client\cfg

In früheren Versionen von CA SSO verwiesen die Einträge "IdentityFile" und "TrustFile" auf Dateien am folgenden Speicherort:

<Installationsordner>\ca\etrust sso\client\cfg

Wenn Sie von früheren Versionen von CA SSO auf r12 aktualisieren, werden die Informationen in den INI-Dateien der früheren Versionen in die INI-Dateien von CA SSO r12 migriert. Daher verweisen die Einträge für "IdentityFile" und "TrustFile" in CA SSO r12 nach dem Upgrade auf den Konfigurationsordner der früheren Versionen. Aus diesem Grund kann der Client nach einem Upgrade keine Verbindung zu einem Windows-Authentifizierungsagenten herstellen.

Bearbeiten Sie nach dem Upgrade auf r12 die Einträge "IdentityFile" und "TrustFile" im Abschnitt [Auth.Win] der Datei Auth.ini manuell, damit sie den Pfad des Clientkonfigurationsordners für r12 angeben.

Ändern der Installationspfade von Antwortdateien

Für ein unbeaufsichtigtes Upgrade müssen sich die Installationspfade für Antwortdateien von CA SSO-Komponenten (Clients, Authentifizierungsagenten und Kennwortsynchronisierungs-Agenten) von den für frühere Versionen angegebenen Installationspfaden unterscheiden.

Kapitel 7: Bekannte Probleme

Dieses Kapitel enthält folgende Themen:

SSO-Server

Folgendes sind bekannte Probleme beim SSO-Server.

Online-Aktualisierungen des CA SSO-Servers werden nach selang-Aktualisierungen nicht geladen

Problem:

Bei der Aktualisierung einer großen Anzahl von Objekten in der Datenbank über ein selang-Batch-Skript werden manche Online-Aktualisierungen des SSO-Servers möglicherweise nicht geladen.

Lösung:

Um dieses Problem zu umgehen und sicherzustellen, dass die neuen Informationen vollständig in den SSO-Server geladen werden, müssen Sie den Serverdienst nach Beendigung der selang-Aktualisierungen erneut starten.

CA Directory-Fehler beim CA SSO-Server-Start

Problem:

Bei einer großen Datenmenge in CA Directory können die folgenden Fehler in der Startphase gemeldet werden:

Nicht genügend Arbeitsspeicher. Inaktivierter Cache.

CA Directory deaktiviert das Caching und kann beim Versuch, die nächste Anforderung zu verarbeiten, abstürzen.

Lösung:

Um dieses Problem zu lösen, sollten Sie das Caching deaktivieren, indem Sie den folgenden Parameter in der PS DSA dxi-Datei festlegen:

set lookup-cache=false

Deinstallation des CA SSO-Servers kann fehlschlagen

Problem:

Der Deinstallationsprozess für den SSO-Server kann wegen zu wenig Speicherplatz im temporären Verzeichnis fehlschlagen.

Lösung:

Stellen Sie sicher, dass das temporäre Verzeichnis mindestens 100 MB freien Speicherplatz aufweist.

Datenmigrationstools für CA SSO-Server unterstützen nur englische Zeichen aus älteren Versionen von CA SSO als r12

Die Datenmigrationstools für SSO-Server unterstützen nur die Migration von Daten, die Zeichen der Ländereinstellung Englisch enthalten, aus älteren Versionen von CA SSO als CA SSO r12.

Active Directory-Objektbeschränkungen auf Microsoft Windows-Plattformen betreffen den CA SSO-Server

Es besteht eine Beschränkung auf 1000 Objekte für Active Directory unter Windows 2000 und auf 1500 Objekte für Active Directory unter Windows 2003. Diese Beschränkungen wirken sich in mehrerlei Hinsicht auf CA SSO aus. Die folgenden Probleme betreffen Konfigurationen, die Active Directory als primären SSO-Benutzerdatenspeicher verwenden:

- Wenn eine Benutzergruppe mehr als 1000 Mitglieder in Active Directory unter Windows 2000 oder mehr als 1500 Mitglieder in Active Directory unter Windows 2003 umfasst, kann Policy Manager nicht alle Benutzer anzeigen, die Mitglied dieser Gruppe sind.
- Das Dienstprogramm psbgc berechnet Cache-Dateien für Hintergrundanwendungslisten nicht für alle Benutzer in einer Gruppe, wenn diese Gruppe mehr als 1000 Mitglieder in Active Directory unter Windows 2000 oder mehr als 1500 Mitglieder in Active Directory unter Windows 2003 umfasst.
- Wenn ein Benutzer Mitglied von mehr als 1000 Benutzergruppen in Active Directory unter 2000 oder mehr als 1500 Benutzergruppen in Active Directory unter Windows 2003 ist, werden nicht alle diese Gruppen zu Berechtigungszwecken herangezogen. Somit kann einem Benutzer der Zugriff auf SSO-Anwendungen verweigert werden (d. h., diese Anwendungen werden nicht in der Anwendungsliste eines Benutzers angezeigt), auch wenn explizite Berechtigungsregeln einigen der Benutzergruppen, in denen der Benutzer Mitglied ist, Zugriff auf diese Anwendungen gewähren.

Hinweis: Diese Einschränkung basiert auf der durch die Einstellung MaxPageSize von Microsoft Active Directory definierten Einschränkung. MaxPageSize wird in Knowledge Base-Artikel 315071 (http://support.microsoft.com/kb/315071) erwähnt.

Keine Anmeldung am SSO-Server aus Policy Manager nach Änderung zur Ausführung im FIPS-Modus möglich

Problem:

Nach dem Upgrade von einem r8.1-CA SSO-Server (mindestens CR6) auf r12 und Änderung des Serverbetriebsmodus in den FIPS-Modus können Sie sich nicht mehr mit Administratorkonten bei Policy Manager anmelden.

Lösung:

Setzen Sie das Administratorkennwort nach dem Upgrade zurück.

Beim CA SSO-Serverdienst tritt nach einem Neustart ein EventLog-Fehler auf

Problem:

Ich erhalte den folgenden Fehler, wenn ich meinen Computer, auf dem der CA SSO-Server installiert ist, neu starte:

Mindestens ein Dienst oder Treiber ist beim Systemstart fehlgeschlagen. Überprüfen Sie das Ereignisprotokoll in der Ereignisanzeige.

Für den vorhergehenden Fehler in der Ereignisanzeige wird folgende Beschreibung angezeigt:

Der CA Single Sign-On-Serverdienst wurde nicht ordnungsgemäß gestartet.

Lösung:

Ignorieren Sie die Fehlermeldung, und starten Sie die CA SSO-Dienste.

Policy Manager

Folgendes sind bekannte Probleme beim SSO Policy Manager.

Alternative Sprachen nicht unterstützt

Policy Manager stellt Optionen zur Installation in einer der folgenden Sprachen zur Verfügung:

- Englisch
- Japanisch
- Chinesisch (Vereinfacht)
- Koreanisch

Es darf jedoch nur Englisch verwendet werden. Japanisch, Chinesisch (Vereinfacht) und Koreanisch werden nicht unterstützt.

Authentifizierungsagenten

Folgendes sind bekannte Probleme bei den SSO-Authentifizierungsagenten.

Schlüsselwort <auto> beim Windows-Authentifizierungs-Host verursacht Fehler

Die Verwendung des Schlüsselworts <auto> beim Authentifizierungs-Host funktioniert nicht, wenn die Eigenschaft "PDCFallback" der Windows-Authentifizierungsmethode auf "No" festgelegt ist. Auch im Erfolgsfall protokolliert der Client einen Fehler, da der Authentifizierungs-Host <auto> nicht gefunden wurde.

Portkonflikt bei den Authentifizierungsagenten

Aus Leistungsgründen verhindern Authentifizierungsagenten die Socket-Wiederverwendung bei ihren Empfangsports nicht. Wenn Administratoren mehrere Instanzen eines Authentifizierungsagenten konfigurieren, die auf einem Computer ausgeführt werden sollen, müssen sie sicherstellen, dass diese nicht beim selben Port empfangsbereit sind.

Dialogfelder für SSO-Authentifizierungsmethoden nicht abgebrochen

Problem:

Die SSO-Authentifizierungsmethode überprüft, dass keine Benutzernamen und Kennwörter mit mehr als 254 Zeichen eingegeben werden. Das zugehörige Warnungsdialogfeld wird nicht immer abgebrochen, wenn CA SSO mit dem Menüpunkt "Beenden" beendet wird oder wenn ein Benutzer als Teil der SSO-GINA-Workstation-Entsperrung geändert wird.

Lösung:

Schließen Sie dieses Dialogfeld und andere zugehörige Dialogfelder, die nicht automatisch geschlossen werden.

Keine Benachrichtigung, wenn die Windows-Authentifizierung fehlschlägt

Wenn Sie die Windows-Authentifizierungsmethode verwenden, AutoNetworkAuth=yes angeben und die Authentifizierung aus einem anderen Grund fehlschlägt, als dass der Host offline ist (etwa, weil Ihr Kennwort abgelaufen ist), werden Sie nicht über den Fehler informiert. Es sieht so aus, als wäre die Authentifizierung nicht durchgeführt worden.

Zertifikatauthentifizierung funktioniert nicht, wenn sich der SSO-Client im Nur-FIPS-Betriebsmodus befindet

Problem:

Die Zertifikatauthentifizierung funktioniert nicht, wenn sich der SSO-Client im Nur-FIPS-Betriebsmodus befindet, weil das PKCS#12-Zertifikat und die PBE-Zertifikate, die für die Authentifizierung verwendet werden, nicht FIPS-kompatibel sind.

Lösung:

Wenn ein Zertifikatauthentifizierungsagent verwendet werden muss, muss der SSO-Client im Nicht-FIPS- oder TLS-Betriebsmodus installiert werden. Im TLS-Modus müssen PKCS-Zertifikate, die mit den FIPS-kompatiblen Algorithmen generiert werden, zur ordnungsgemäßen Authentifizierung verwendet werden.

Interpreter

Folgendes sind bekannte Probleme beim Interpreter.

Lycos und Hotbot funktionieren nicht mit der Erweiterung "sso html_search"

Die Suchmaschinen Lycos und Hotbot funktionieren nicht mit der Interpreter-Erweiterung sso html_search.

Fehler bei Erweiterung SSO Waittext

Wenn der Text, auf den "sso waittext" wartet, im Zielfenster ausgewählt wird, schlägt "sso waittext" fehl und wird eine Fehlermeldung angezeigt.

Session Administrator (Sitzungsadministrator)

Folgendes sind bekannte Probleme beim Session Administrator (Sitzungsadministrator).

Internetverknüpfung wird in Mozilla oder Firefox nicht erstellt

Problem:

Die Internetverknüpfung für Session Administrator (Sitzungsadministrator) wird in Mozilla- oder Firefox-Lesezeichen nicht erstellt, wenn Mozilla oder Firefox als Standardbrowser verwendet wird.

Lösung:

Importieren Sie die Internetverknüpfung für Session Administrator (Sitzungsadministrator) aus den Favoriten von Microsoft Internet Explorer in Mozilla- oder Firefox-Lesezeichen.

Navigieren im interaktiven Modus

Problem:

Wenn Sie die Installation im interaktiven Modus durchführen, die Anzeige des Speicherorts für die Installation verlassen und dann zurück zu dieser Anzeige navigieren und den Speicherort für die Installation ändern, werden alle Informationen, die Sie bei der Installation eingegeben haben, auf die Standardwerte zurückgesetzt.

Lösung:

Geben Sie alle Werte erneut ein.

Unterstützung für FIPS

Der Session Administrator (Sitzungsadministrator) unterstützt FIPS 140-2 nicht. Um den Session Administrator (Sitzungsadministrator) zu verwenden, installieren Sie den CA SSO-Server in einem Nicht-FIPS-Modus oder einem gemischtem Modus.

IPv6-Netzwerkfunktionen nicht unterstützt

Problem:

Der Session Administrator (Sitzungsadministrator) unterstützt keine IPv6-Netzwerkfunktionen.

Lösung:

Um den Session Administrator (Sitzungsadministrator) zu verwenden, aktivieren Sie die IPv4-Kommunikation für Systeme, auf denen der SSO-Server und der SSO Session Administrator (SSO-Sitzungsadministrator) installiert sind.

Kennwortsynchronisierungs-Agent (PSA)

Folgendes sind bekannte Probleme beim Kennwortsynchronisierungs-Agenten (PSA).

PSA-Funktionen zum Ändern/Reparieren der Installation nicht verfügbar

Problem:

Die PSA-Funktionen zum Ändern/Reparieren der Installation sind nicht verfügbar.

Lösung:

Entfernen Sie die frühere Version des Windows-PSA (Password Synchronization Agent, engl. für Kennwortsynchronisierungs-Agent) mit Hilfe der Windows-Funktion "Software", und installieren Sie dann den PSA von r12 erneut.

Application Wizard (Anwendungsassistent)

Folgendes sind bekannte Probleme beim Application Wizard (Anwendungsassistenten).

Satzzeichen dürfen in Anwendungsfenstern und -seiten nicht verwendet werden

Ihr Automatisierungsskript kann Anwendungsfenster und -seiten nicht richtig identifizieren, wenn Satzzeichen verwendet werden, um das Anwendungsfenster oder die Anwendungsseite anzugeben. Verwenden Sie keine Satzzeichen, um Anwendungsfenster und -seiten anzugeben.

Für Windows-Anwendungen:

- Ermitteln Sie Satzzeichen im Fenstertitel, die verhindern können, dass Ihr Automatisierungsskript das Fenster findet.
- Ersetzen Sie im Dialogfeld "Automating windows" (Fenster automatisieren) Satzzeichen in den Titel- oder Textfeldern durch das Platzhalterzeichen "*" (Stern).

Für browserbasierte Anwendungen:

- Ermitteln Sie Satzzeichen im Seitentitel, die verhindern können, dass Ihr Automatisierungsskript die Webseite findet.
- Verwenden Sie im Dialogfeld "Automating forms" (Formulare automatisieren) im Feld "Page Title" (Seitentitel) nur den Teil des Seitentitels, der keine Satzzeichen enthält.

- Verwenden Sie im Feld "Unique Text" (Eindeutiger Text) nur alphanumerische Zeichen und Leerzeichen.

Verwenden Sie nur Standard-Steuerelementtypen beim automatisierten Fenster

Problem:

Der Application Wizard (Anwendungsassistent) kann manche Steuerelemente beim automatisierten Fenster nicht erkennen, wenn in der Windows-Anwendung nicht nur Standard-Steuerelementtypen verwendet oder eigene GUI-Elemente gerendert werden.

Lösung:

Gehen Sie wie folgt vor, wenn ein Steuerelement in der Steuerelementtabelle unten im Dialogfeld "Automating window" (Fenster automatisieren) nicht angezeigt wird:

- Aktivieren Sie das Kontrollkästchen "Show All" (Alle anzeigen).
- Untersuchen Sie die Tabelle, um zu ermitteln, ob das Steuerelement als unbekannter Steuerelementtyp aufgeführt wurde, und weisen Sie ihm eine Aktion zu.

Hinweis: Diesen Steuerelementtypen können Sie nur die Aktionen "Click" (Klicken), "Click exact point" (Auf exakte Stelle klicken) und "Type other text" (Weiteren Text eingeben) zuweisen.

SSO-Client

Folgendes sind bekannte Probleme beim SSO-Client.

Dialogfelder werden nicht geschlossen

Problem:

Manche Dialogfelder von Drittanbietern werden nicht immer abgebrochen, wenn CA SSO mit dem Menüpunkt "Beenden" beendet wird oder wenn ein Benutzer als Teil der SSO-GINA-Workstation-Entsperrung geändert wird.

Lösung:

Schließen Sie diese Dialogfelder und andere zugehörige Dialogfelder, die nicht automatisch geschlossen werden.

Aufgeführte Server gering halten

Problem:

Der SSO-Client braucht länger, um einen Benutzer zu authentifizieren und Anwendungen zu starten, wenn im aktuellen Serversatz zahlreiche Hostnamen angegeben sind.

Lösung:

Halten Sie die Anzahl der in Ihrem Serversatz aufgeführten Server gering, und meiden Sie Hostnamen, die derzeit nicht aufgelöst werden können.

Kontextmenü der Taskleiste funktioniert nicht, wenn der Startbereich angedockt wird

Problem:

Wenn der Startbereich angedockt wird, funktioniert das Kontextmenü nicht.

Lösung:

Docken Sie den Startbereich aus.

Taskleistensymbol wird nicht ausgeblendet, wenn die Startbereichsawendung beendet wird

Problem:

Wenn Sie die Startbereichsanwendung beenden, wenn diese angedockt ist, wird das Taskleistensymbol nicht sofort ausgeblendet.

Lösung:

Klicken Sie auf das Taskleistensymbol.

Bildschirmgröße des Startbereichs wird nicht automatisch angepasst

Problem:

Die Breite des angedockten Startbereichs wird als Prozentsatz der Bildschirmgröße bestimmt. Wenn Sie die Bildschirmauflösung ändern, wird der Startbereich nicht automatisch entsprechend angepasst. Sie sehen deshalb nicht den ganzen Startbereich, wenn Sie die Bildschirmauflösung verringern.

Lösung:

Passen Sie die Größe des Startbereichs an, nachdem die Auflösung geändert wurde.

Größe des Startbereichs wird nicht ordnungsgemäß geändert

Wenn Sie die automatische Schaltflächengröße (ButtonSize=auto) in der Datei Client.ini konfigurieren, wird die Größe des Startbereichs beim Abmelden nicht erwartungsgemäß geändert.

Anwendungsnamen können abgeschnitten werden

Anwendungsnamen können abgeschnitten und ein sinnloses Zeichen am Ende angehängt werden, wenn sehr lange Anwendungsnamen verwendet werden.

Ereignisbefehle können sowohl in lokalen Sitzungen als auch in Remote-Sitzungen ausgeführt werden

Wenn eine Remote Desktop-Verbindung verwendet wird, um auf den lokalen Host zuzugreifen, werden die SSO-Ereignisbefehle zum An- und Abmelden möglicherweise sowohl in der lokalen Sitzung als auch in der Remote-Sitzung ausgeführt.

Navigieren im interaktiven Modus

Problem:

Wenn Sie die Installation im interaktiven Modus durchführen, die Anzeige des Speicherorts für die Installation verlassen und dann zurück zu dieser Anzeige navigieren und den Speicherort für die Installation ändern, werden alle Informationen, die Sie bei der Installation eingegeben haben, auf die Standardwerte zurückgesetzt.

Lösung:

Geben Sie alle Werte erneut ein.

Remote Desktop-Anmeldung für GINA und Anmeldeinformationsanbieter schlägt fehl

Die Remote Desktop-Anmeldung für GINA und Anmeldeinformationsanbieter schlägt das erste Mal fehl, wenn vor der Remote-Anmeldung eine lokale Anmeldung an der Workstation erfolgt.

Kapitel 8: Unterstützte Produktsprachen

Ein *internationalisiertes* Produkt ist eine englische Version, die unter den erforderlichen Betriebssystemen und den erforderlichen Produkten anderer Hersteller in anderen Sprachen korrekt ausgeführt wird und die Eingabe und Ausgabe von Daten in der entsprechenden Sprache unterstützt. Bei internationalisierten Produkten können auch Konventionen der jeweiligen Sprache für Datum, Uhrzeit, Währung und Zahlenformat angegeben werden.

Ein *übersetztes* Produkt (manchmal auch *lokalisierte* Version genannt) ist ein internationalisiertes Produkt, dessen Benutzeroberfläche, Online-Hilfe und Dokumentation in der jeweiligen Landessprache vorliegen und das die entsprechenden Formate für Datum, Uhrzeit, Währung und Zahlen dieser Sprache unterstützt.

CA SSO wurde internationalisiert und kann nun auf nicht englischsprachigen Plattformen ausgeführt werden. Übersetzt wurden jedoch nur der CA SSO-Client und das CA SSO-Installationsprogramm, und zwar in die folgenden Sprachen:

- Französisch
- Deutsch
- Italienisch
- Spanisch

Hinweis: Falls Sie das Produkt in einer Sprachumgebung ausführen, die *nicht* in der Tabelle aufgeführt ist, können Probleme auftreten.

Kapitel 9: Funktionen zur behindertengerechten Bedienung

CA ist es ein Anliegen, sicherzustellen, dass alle Kunden, unabhängig von ihrer körperlichen Unversehrtheit, die Produkte und zugehörige Dokumentation von CA zur Erledigung wichtiger Geschäftsaufgaben verwenden können. In diesem Abschnitt werden die Funktionen zur behindertengerechten Bedienung beschrieben, die Bestandteil von CA SSO sind.

Hinweis: Weitere Informationen zu den Initiativen von CA zur behindertengerechten Bedienung finden Sie auf der Website www.ca.com.

Dieses Kapitel enthält folgende Themen:

Produktverbesserungen

Der SSO-Client bietet Verbesserungen für eine behindertengerechte Bedienung in den folgenden Bereichen:

- Anzeige
- Ton
- Tastatur
- Maus
- Support

Hinweis: Die folgenden Informationen gelten für Windows- und für Macintosh-basierte Anwendungen. Java-Anwendungen können auf vielen Hostbetriebssystemen ausgeführt werden, von denen einige bereits mit Technologien für Bedienungshilfen ausgestattet sind. Damit diese Technologien Zugriff auf in JPL geschriebene Programme bieten können, benötigen Sie eine Bridge zwischen ihren nativen Umgebungen und der Java-Unterstützung für behindertengerechte Bedienung, die in der JVM (Java Virtual Machine) verfügbar ist. Diese Bridge vermittelt zwischen der JVM und der jeweiligen nativen Plattform, unterscheidet sich daher je nach Plattform geringfügig. Sun entwickelt derzeit sowohl die JPL- als auch die Win32-Seite dieser Bridge.

Anzeige

Um die Ablesbarkeit auf dem Computerbildschirm zu verbessern, können Sie die folgenden Optionen anpassen:

- Schriftstil, Farbe und Elementgröße

  Ermöglicht Ihnen die Auswahl der Schriftfarbe, -größe und weiterer visueller Kombinationen.

- Bildschirmauflösung

  Ermöglicht Ihnen, die Pixelanzahl zu ändern, um Objekte auf dem Bildschirm zu vergrößern.

- Cursor-Breite und Blinkrate

  Ermöglicht Ihnen, die Sichtbarkeit des Cursors zu verbessern oder das Blinken des Cursors zu minimieren.

- Symbolgröße

  Ermöglicht Ihnen, Symbole größer zu machen, um die Sichtbarkeit zu verbessern, oder kleiner, um mehr Platz auf dem Bildschirm zu haben.

- Hochkontrastschemas

  Ermöglicht Ihnen, Farbkombinationen auszuwählen, die besser zu sehen sind.

Ton

Verwenden Sie Töne als visuelle Alternative oder um Computersignale besser hörbar oder unterscheidbar zu machen, indem Sie die folgenden Optionen anpassen:

- Volumen

  Ermöglicht Ihnen, Computersignale lauter oder leiser einzustellen.

- Text-zu-Sprache

  Ermöglicht Ihnen, Befehlsoptionen zu hören und sich Texte vorlesen zu lassen.

- Warnungen

  Ermöglicht Ihnen, visuelle Warnungen anzuzeigen.

- Hinweise

  Gibt Ihnen akustische oder visuelle Hinweise, wenn Funktionen für eine behindertengerechte Bedienung aktiviert oder deaktiviert werden.

- Schemas

  Ermöglicht Ihnen, Computersignale bestimmten Systemereignissen zuzuordnen.

- Beschriftungen

  Ermöglicht Ihnen, Titel für Sprache und Töne anzuzeigen.

Tastatur

Sie können die folgenden Tastaturanpassungen vornehmen:

- Wiederholrate

  Ermöglicht Ihnen, festzulegen, wie schnell ein Zeichen wiederholt wird, wenn eine Taste gedrückt wird.

- Töne

  Ermöglicht die Wiedergabe von Tönen, wenn bestimmte Tasten gedrückt werden.

- Sticky Keys

  Wenn eine Tastenkombination gedrückt werden soll, können Sie eine Taste wie UMSCHALT, STRG, ALT oder die Windows-Taste drücken, die dann so lange aktiv bleibt, bis Sie eine weitere Taste drücken.

Maus

Sie können die folgenden Optionen verwenden, um Ihre Maus schneller und einfacher bedienbar zu machen:

- Klickgeschwindigkeit

  Ermöglicht Ihnen, zu wählen, wie schnell eine Maustaste gedrückt werden muss, um eine Auswahl zu treffen.

- Klicksperre

  Ermöglicht Ihnen, Elemente zu markieren oder zu ziehen, ohne die Maustaste gedrückt zu halten.

- Umkehraktion

  Ermöglicht Ihnen, die von der linken und rechten Maustaste gesteuerte Funktion zu tauschen.

- Blinkrate

  Ermöglicht Ihnen, zu wählen, wie schnell der Cursor blinkt bzw. ob er überhaupt blinkt.

- Zeigeroptionen

  Sie haben folgende Möglichkeiten:

  - Zeiger bei der Eingabe ausblenden
  - Position des Zeigers anzeigen
  - Geschwindigkeit festlegen, mit der sich der Zeiger auf dem Bildschirm bewegt
  - Größe und Farbe des Zeigers für verbesserte Darstellung wählen
  - Zeiger in einem Dialogfeld an eine Standardposition bewegen

Support

Sie können die folgenden Optionen verwenden, um SSO-Support zu erhalten.

- Online- und E-Mail-Support

  Ermöglicht Ihnen, Hilfe zu erhalten, wenn Sie schwerhörig sind.

  Hinweis: Der Online-Support ist für Personen mit Sehbehinderung nur teilweise zugänglich.

- Telefonischer Support

  Ermöglicht Ihnen, Hilfe zu erhalten, wenn Sie unter einer Sehbehinderung leiden.

Tastenkombinationen

In der folgenden Tabelle werden die Tastenkombinationen aufgeführt, die SSO unterstützt:

Tastatur	Beschreibung
Strg+X	Ausschneiden
Strg+C	Kopieren
Strg+K	"Weiter suchen"
Strg+F	Suchen und ersetzen
Strg+V	Einfügen
Strg+S	Speichern
Strg+Umschalt+S	Alle speichern
Strg+D	Zeile löschen
Strg+Nach-Rechts	Nächstes Wort
Strg+Nach-Unten	Zeile nach unten
Ende	Zeilenende

Tastenkombinationen

Folgendes sind die SSO-Dialogfelder und die Tastenkombinationen, die für die Steuerelemente verfügbar sind:

Dialogfeld "Anmeldeinformationen festlegen"

- Anmeldename

  Alt+L

- Neues Kennwort

  Alt+N

- Kennwort überprüfen

  Alt+V

- Erweitert

  Alt+A

SSO-Sitzung schließen

- Ausgewählte Sitzung schließen

  Alt+S

- Anmeldung fortsetzen

  Alt+O

- Anmeldung abbrechen

  Alt+C

Meine Anwendungen

- Öffnen

  Alt+O

- Kennwort ändern

  Alt+P

- Startgruppe

  Alt+G

- Desktop

  Alt+D

- Aktualisieren

  Alt+F

Meine Details

- Authentifizierungsdetails ändern

  Alt+A

Erweiterte Kennwortoptionen

- Anmeldeinformationen festlegen

  Alt+L

- Ausstehende Kennwortänderung abbrechen

  Alt+P

Endbenutzer-Lizenzvertrag

- Drucken

  Alt+P

Info zu CA Single Sign-On

- Bekanntmachungen von Drittanbietern

  Alt+T

- Systeminformationen

  Alt+I

- Technischer Support

  Alt+S

Serversatzauswahl

- Serversatz

  Alt+S

- Authentifizierungsmethode

  Alt+A

- Domäne

  Alt+D

- Anmelden

  Alt+L

Serversatzauswahl (GINA-Konfiguration)

- Nur Windows-Anmeldung

  Alt+W

- Abmelden

  Alt+O

- Herunterfahren

  Alt+U

Authentifizierung - SSO

- Benutzername

  Alt+U

- Kennwort

  Alt+P

- Ändern

  Alt+C

- (GINA-Konfigurationssteuerelemente) Domäne

  Alt+D

Anmeldeinformationen ändern - SSO

- Benutzername

  Alt+U

- Altes Kennwort

  Alt+O

- Neues Kennwort

  Alt+N

- Kennwort überprüfen

  Alt+V

- (GINA-Konfigurationssteuerelemente) Domäne

  Alt+D

Authentifizierung - RSA SecurID

- Vorhandener Benutzer

  Alt+E

- Neuer Benutzer

  Alt+N

- Benutzername

  Alt+U

- PIN

  Alt+P

- Token-Code

  Alt+T

- (GINA-Konfigurationssteuerelemente) Domäne

  Alt+D

PIN-Anforderung - RSA SecurID

- Systemgenerierung

  Alt+S

- Benutzergenerierung

  Alt+U

Eingabe von neuer PIN-Nummer - RSA SecurID

- Neue PIN-Nummer

  Alt+N

- PIN bestätigen

  Alt+C

Nächstes Token - RSA SecurID

- Token-Code

  Alt+T

Authentifizierung - LDAP

- Benutzername

  Alt+U

- Kennwort

  Alt+P

- Ändern

  Alt+C

- (GINA-Konfigurationssteuerelemente) Domäne

  Alt+D

Anmeldeinformationen ändern - LDAP

- Benutzername

  Alt+U

- Altes Kennwort

  Alt+O

- Neues Kennwort

  Alt+N

- Kennwort überprüfen

  Alt+V

- (GINA-Konfigurationssteuerelemente) Domäne

  Alt+D

Authentifizierung - Zertifikat

- PKCS#11-Token

  Alt+T

- PKCS#12-Datei

  Alt+M

- Ändern

  Alt+C

- (GINA-Konfigurationssteuerelemente) Domäne

  Alt+D

Zertifikat

- Zertifikat zur Authentifizierung auswählen

  Alt+S

- Details

  Alt+D

Authentifizierung - Windows

- Benutzername

  Alt+U

- Kennwort

  Alt+P

- Ändern

  Alt+C

- (GINA-Konfigurationssteuerelemente) Domäne

  Alt+D

Anmeldeinformationen ändern - Windows

- Benutzername

  Alt+U

- Altes Kennwort

  Alt+O

- Neues Kennwort

  Alt+N

- Kennwort überprüfen

  Alt+V

- (GINA-Konfigurationssteuerelemente) Domäne

  Alt+D

Fehlermeldungsfeld

- Ja

  Alt+Y

- Nein

  Alt+N

- "Wiederholen"

  Alt+R

- Details

  Alt+D

Sperrung des Computers aufheben

- Benutzername

  Alt+U

- Kennwort

  Alt+O

- Domäne

  Alt+D

Bei Windows abmelden

- Abmelden

  Alt+L

- Nein

  Alt+N

Bei Windows anmelden

- Benutzername

  Alt+U

- Kennwort

  Alt+O

- Domäne

  Alt+D

- Herunterfahren

  Alt+S

CA Single Sign-On-Sicherheit

- Computer sperren

  Alt+K

- Abmelden

  Alt+L

- Herunterfahren

  Alt+S

- Kennwort ändern

  Alt+C

- Aufgaben-Manager

  Alt+T

Kennwort ändern (Windows)

- Benutzername

  Alt+U

- Domäne

  Alt+D

- Altes Kennwort

  Alt+O

- Neues Kennwort

  Alt+N

- Neues Kennwort bestätigen

  Alt+C

Computer herunterfahren

- Was soll der Computer tun?

  Alt+W

Die verfügbaren Kontextmenüeinträge und Tastenkombinationen lauten wie folgt:

- Anmelden

  Alt+N

- Abmelden

  Alt+F

- Anwendungsliste aktualisieren

  Alt+R

- Anwendungen

  Alt+A

- SSO-Tools öffnen

  Alt+T

- Startbereich öffnen

  Alt+L

- Computer sperren

  Alt+C

- Info zu

  Alt+B

- Beenden

  Alt+E

Kapitel 10: Bookshelf

Der Bookshelf ermöglicht den Zugriff auf die gesamte Dokumentation von CA SSO von einem zentralen Ort aus. Der Bookshelf enthält Folgendes:

- Eine gemeinsame, erweiterbare Inhaltsliste für alle Handbücher im HTML-Format
- Volltextsuche über alle Handbücher mit bewerteten Suchergebnissen und im Inhalt hervorgehobenen Suchbegriffen
- Klickelemente ("Brotkrümel"), die zu übergeordneten Themen führen
- Gemeinsamer Index für alle Handbücher
- Links auf PDF-Versionen der Handbücher zum Drucken

Zum Anzeigen des Bookshelfs ist Internet Explorer 6 bzw. 7 oder Mozilla Firefox 2 erforderlich. Für die Bookshelf-Links zu PDF-Handbüchern, die ausgedruckt werden können, ist Adobe Reader 7 oder 8 erforderlich. Sie können unter www.adobe.com eine unterstützte Version von Adobe Reader herunterladen.

Für dieses Produkt gibt es folgende Handbücher im PDF-Format:

- Administrationshandbuch
- Online-Hilfe für den CA SSO-Client
- Implementierungshandbuch
- Hilfe für den CA SSO Policy Manager
- Versionshinweise
- Handbuch für TCL-Skripts

Verwenden des Bookshelfs

1. Suchen und öffnen Sie den Dokumentationsordner im Produktinstallationsordner.
2. Öffnen Sie den Bookshelf wie folgt:
   - Öffnen Sie die Datei "Bookshelf.hta", wenn sich der Bookshelf auf dem lokalen System befindet und Sie Internet Explorer verwenden.
   - Öffnen Sie die Datei "Bookshelf.html", wenn sich der Bookshelf auf einem Remote-System befindet, oder wenn Sie Mozilla Firefox verwenden.

Kapitel 11: Veröffentlichte Programmkorrekturen

Die vollständige Liste veröffentlichter Programmkorrekturen für dieses Produkt ist über "Published Solutions" auf der Seite "CA Online Support" erhältlich.

Anhang A: Drittanbieter-Lizenzen

Dieses Kapitel enthält folgende Themen:

Apache License Version 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions. "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

   "Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   a. You must give any other recipients of the Work or Derivative Works a copy of this License; and

   b. You must cause any modified files to carry prominent notices stating that You changed the files; and

   c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   d. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License.

   You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text must be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

ActiveState Community License

This product includes software known as TCL. The TCL software is distributed in accordance with the following license agreement:

This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. government, the Government shall have only "Restricted Rights" in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

Definitions:

"ActiveState" refers to ActiveState Corp., the Copyright Holder of the Package.

"Package" refers to those files, including, but not limited to, source code, binary executables, images, and scripts, which are distributed by the Copyright Holder.

"You" is you, if you are thinking about copying or distributing this Package.

Terms:

1. You may use this Package for commercial or non-commercial purposes without charge.
2. You may make and give away verbatim copies of this Package for personal use, or for use within your organization, provided that you duplicate all of the original copyright notices and associated disclaimers. You may not distribute copies of this Package, or copies of packages derived from this Package, to others outside your organization without specific prior written permission from ActiveState (although you are encouraged to direct them to sources from which they may obtain it for themselves).
3. You may apply bug fixes, portability fixes, and other modifications derived from ActiveState. A Package modified in such a way shall still be covered by the terms of this license.
4. ActiveState's name and trademarks may not be used to endorse or promote packages derived from this Package without specific prior written permission from ActiveState.

5. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Boost Software License Version 1.0

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Zlib V1.2.3

This product includes zlib developed by Jean-loup Gailly and Mark Adler.